

On the problem of non-zero word error rates for fixed-rate error correction codes in continuous variable quantum key distribution

Sarah J. Johnson,^{1,*} Andrew M. Lance,² Lawrence Ong,¹
Mahyar Shirvanimoghaddam,¹ T. C. Ralph,³ and Thomas Symul²

¹*School of Electrical Engineering and Computer Science, The University of Newcastle, Australia*

²*QuintessenceLabs Pty. Ltd., Canberra ACT, Australia.*

³*Centre for Quantum Computation and Communication Technology,
School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia*

The maximum operational range of continuous variable quantum key distribution protocols has shown to be improved by employing high-efficiency forward error correction codes. Typically, the secret key rate model for such protocols is modified to account for the non-zero word error rate of such codes. In this paper, we demonstrate that this model is incorrect: Firstly, we show by example that fixed-rate error correction codes, as currently defined, can exhibit efficiencies greater than unity. Secondly, we show that using this secret key model combined with greater than unity efficiency codes, implies that it is possible to achieve a positive secret key over an entanglement breaking channel - an impossible scenario. We then consider the secret key model from a post-selection perspective, and examine the implications for key rate if we constrain the forward error correction codes to operate at low word error rates.

INTRODUCTION

Quantum key distribution is one of the most advanced applications of quantum physics and information science. It enables the distribution of information-theoretically secure random key material between two parties in spatially-separated locations connected by an unsecured optical link [1].

There are two complementary approaches to quantum key distribution: discrete variable quantum key distribution uses single-photon or weak coherent states and single photon detectors [2], while continuous variable quantum key distribution (CVQKD) uses coherent or squeezed states of light and homodyne detectors [3]. Both discrete and continuous quantum key distribution systems have been demonstrated (for a review see [4]) and importantly both the discrete and continuous approaches to quantum key distribution have been proven to be information-theoretic secure, the latter against collective attacks [5, 6] and with composable security [7].

Continuous variable quantum key distribution has gained interest recently because of the potential technology advantages it offers that may enable higher secret key rates. Technological advantages include high-quantum efficiency homodyne detectors; high-speed commercial-off-the-shelf optical components and compatibility with optical network infrastructure.

Originally limited to short distances [8], the operation range of CVQKD protocols was considerably extended by employing the reverse reconciliation protocol that exploits one-way communication, including forward error correction codes in the error reconciliation post processing step [9]. Low density parity check (LDPC) and multi-edge LDPC (ME-LDPC) codes are examples of high-efficiency forward error correction codes that have been employed in CVQKD systems [10–15]. The ME-LDPC

codes in particular exhibit good error correction performances at low signal-to-noise (SNR) ratios, making them suitable for CVQKD applications.

A simple and useful model for the secret key rate of CVQKD protocols in the case of collective attacks can be derived when one assumes a specific reconciliation procedure. Specifying the reconciliation procedure to be forward error reconciliation, the secret key rate can then be empirically modeled by [16]

$$\Delta I = \beta I_{AB} - I_E \quad (1)$$

where I_E denotes the bound on an eavesdropper's (Eve's) maximum accessible information, I_{AB} denotes the capacity of the channel between the sender (Alice) and the receiver (Bob), and β denotes the efficiency of reconciliation.

The model for the secret key rate in Eq. (1) is commonly used in the literature to compare the performance of CVQKD protocols under varying conditions, for example, different amounts of loss and noise. Importantly, Eq. (1) assumes that every codeword of the forward error correction code is decoded correctly.

Practical applications of ME-LDPC and LDPC codes inherently exhibit a non-zero word error rate (WER) [10, 17]. The WER is the rate at which the decoder fails to decode the correct codewords. Since the adoption of forward error correction codes in CVQKD systems, the model of the secret key rate has been subsequently modified to include the efficiency and WER of the code [10, 15]

$$\Delta I = (\beta I_{AB} - I_E)(1 - p_{\text{fail}}) \quad (2)$$

where p_{fail} is the rate at which the decoder fails to decode to a valid codeword. We point out that it is not clear if this secret key model was formally derived. We also note that for all error correction schemes there is always a

non-zero probability that a valid, but incorrect, codeword could be returned. I.e. the decoder will fail but will not know that it has failed. This would not be detected by Alice and Bob, resulting in an incorrect secret key which would not be discovered until the key is used. In our simulations, we have used the true word error rate (as we have knowledge of the transmitted message so can detect all failures). In practice, this won't be possible, however it is usually assumed that the undetected error rate is negligible.

In this paper we show that the current key model Eq. (2) is incorrect. Firstly, we demonstrate that fixed-rate error correction codes can exhibit efficiencies, β greater than unity for a range of word error rates. Secondly, we show that by using the secret key model Eq. (2) combined with β greater than unity, it is possible to achieve a positive secret key over an entanglement breaking channel. We then consider the secret key model from a CVQKD post-selection perspective, and also examine the implications for key rate if we constrain the forward error correction codes to operate at low word error rates.

FORWARD ERROR CORRECTION CODES WITH β GREATER THAN UNITY

Since the adoption of forward error correction codes in CVQKD protocols, the model for secret key rate has been formulated to account for the non-ideal performance of the forward error correction coding scheme. The two sources of this non-ideal performance are 1) the losses due to mapping a binary error correction code onto a Gaussian-input channel, and 2) the losses due to the performance of a practical error correction code compared to the ideal, capacity achieving, error correction code.

It has been shown [18] that entanglement-based CVQKD protocols are equivalent to so-called prepare-and-measure CVQKD protocols where Alice transmits Gaussian modulated coherent states. In the latter case, if the sender encodes with Gaussian signals, a mapping protocol can be used to transform the Gaussian symbols to binary symbols for subsequent error correction. Recent advances have been made on efficient mapping protocols (for example see [19] and references therein), which have been shown to be highly efficient for low SNR ratios, typically required for CVQKD protocols [19]. We denote the efficiency of the mapping protocol, compared to perfect Gaussian mapping by β_{MAP} . This mapping efficiency, although important, is not the focus of this paper.

Following the mapping step, reconciliation is then performed using an error correction code designed for the binary-input additive Gaussian white noise (BI-AWGN) channel, in particular LDPC [10, 11] and ME-LDPC codes [12–15].

The efficiency of the forward error correction code is

calculated according to [10, 13, 16]

$$\beta_{\text{FEC}} = \frac{R}{I_{\text{AB}}} \quad (3)$$

where $R = k/n$ is the rate of the error correction code that maps a k bit message to an n bit codeword, and I_{AB} denotes the capacity of the channel between the sender (Alice) and the receiver (Bob), i.e. the rate of the ideal capacity-achieving code. The total efficiency of the reconciliation scheme is then

$$\beta = \beta_{\text{MAP}} \beta_{\text{FEC}}. \quad (4)$$

In the remainder of this paper we will assume that $\beta_{\text{MAP}} = 1$. Substituting Eq. (3) into Eq. (2) we see that the key rate for a rate $R = k/n$ forward error correction code operating at a WER of p_{fail} can be calculated as

$$\Delta I = (R - I_{\text{E}})(1 - p_{\text{fail}}). \quad (5)$$

For LDPC and ME-LDPC codes, the code performance at a given SNR (where the SNR is determined by the parameters of the CVQKD protocol model) can be determined theoretically by evaluating the expected performance of an ensemble of infinite length codes with a particular structure using density evolution [20]. Density evolution returns the *threshold* of a rate R code ensemble, which is the smallest SNR at which the BER, the fraction of codeword bits remaining in error following decoding, goes to zero as decoding proceeds. For a given SNR, we find the highest code rate R with a threshold at or below that SNR. Then β is [13]

$$\beta_{\text{FEC}} = \frac{R}{I_{\text{AB}}(s_{\text{th}})} \quad (6)$$

where $I_{\text{AB}}(s_{\text{th}})$ is the rate of the capacity achieving code on an AWGN channel with SNR equal to s_{th} . The secret key rate model with a rate R code with threshold s_{th} is

$$\Delta I = R - I_{\text{E}}(s_{\text{th}}), \quad (7)$$

where $I_{\text{E}}(s_{\text{th}})$ is the bound on the information leaked to Eve with SNR equal to s_{th} and the WER is zero. By the definition of the threshold, the code operates at a zero error rate and consequently $R \leq I_{\text{AB}}(s_{\text{th}})$ follows from the channel coding theory and so $\beta_{\text{FEC}} \leq 1$.

In contrast, for any finite length code, the error rate is bounded away from zero. Instead, the performance of finite-length error correction codes can be determined via simulation to find the error rate curves (BER and WER) for a particular code as the SNR is varied. Since the error rate decreases as the SNR is increased, the SNR value at which a given code will be operated, s_{op} , will depend on the WER that can be tolerated by the application. Thus the rate R of the error correction code we can employ on a given channel will depend on the WER we allow.

For example, the rate 0.02 code in [13] has a theoretical threshold (found using density evolution) of $s_{\text{th}} = 0.02865$. Consequently,

$$\beta_{\text{FEC}} = \frac{R}{I_{\text{AB}}(s_{\text{th}} = 0.02865)} = \frac{0.02}{0.02038} = 0.981, \quad (8)$$

and the secret key rate model with SNR $s = 0.02865$ is

$$\Delta I = 0.02 - I_{\text{E}}(s = 0.02865). \quad (9)$$

In practice, a length 2^{20} rate 0.02 code operating at an SNR of $s = 0.029$ has a WER of $1/3$ [13]. Applying Eq. (3), this gives

$$\beta_{\text{FEC}} = \frac{R}{I_{\text{AB}}(s_{\text{op}} = 0.029)} = \frac{0.02}{0.02062} = 0.97, \quad (10)$$

The secret key rate model for this code operating at a WER of $1/3$ with SNR $s = 0.029$ is

$$\Delta I = 2/3(0.02 - I_{\text{E}}(s = 0.029)). \quad (11)$$

If we take the practice of allowing non-zero WERs to the extreme, it is possible to significantly increase the rate R we can operate at a given SNR, s to above $I_{\text{AB}}(s)$, or equivalently, to operate at a β above 1. For example, Fig. 1 shows the finite length performance of a rate 0.02 code with degree-distribution from [13] when the code length is 10^5 bits and a maximum of 5,000 decoder iterations are allowed. By allowing a WER of 0.9999, one can operate with rate 0.02 at an SNR of 0.0258 and thus

$$\beta_{\text{FEC}} = \frac{R = 0.02}{I_{\text{AB}}(s_{\text{op}} = 0.0258)} = \frac{0.02}{0.018374} = 1.09. \quad (12)$$

The secret key rate model for this code operating at a WER of 0.9999 with SNR $s = 0.0258$ is

$$\Delta I = 0.00001(0.02 - I_{\text{E}}(0.0258)). \quad (13)$$

For the same code rate, R , increasing the WER has allowed us to reduce s and thus reduce $I_{\text{E}}(s)$. Consequently, the current secret key rate model informs us that by increasing the WER we are able to increase the range of s for which the same rate R code can operate.

Also shown in Fig. 1 is the Shannon capacity result for rate 0.02 codes and we can see that the ME-LDPC code is in fact operating at an SNR below the Shannon channel capacity which is why β can be calculated as greater than 1. Of course this code is not outperforming the Shannon channel capacity, rather the comparison is not valid. Coding schemes with a non-zero error rate are not bound by the same capacity formula as schemes with a zero error rate. It is well known that the capacity of the AWGN channel varies as the BER is allowed to increase [21]. If the BER is below 10^{-4} the effect is insignificant [21], however, above this, the SNR required to decode

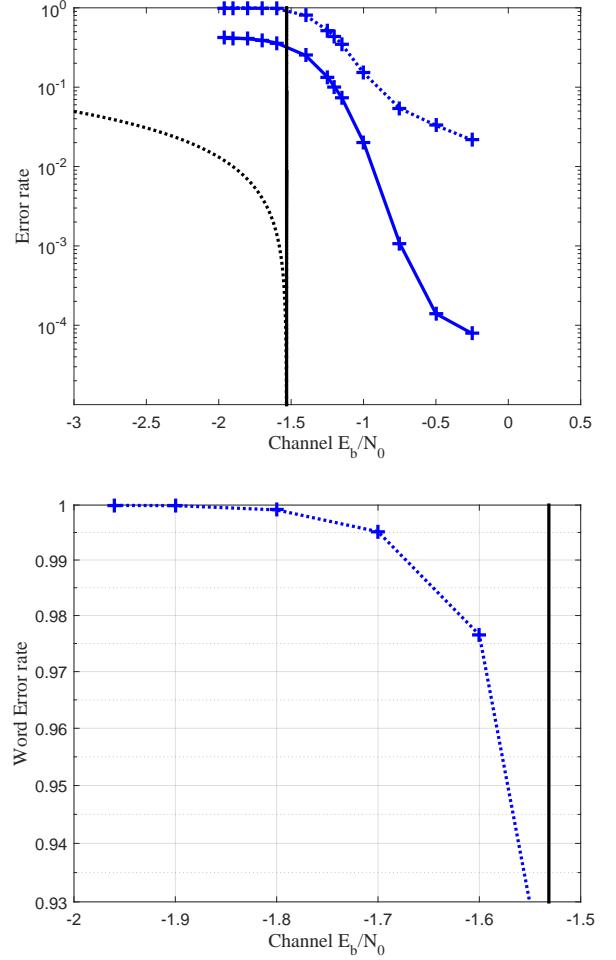


FIG. 1. BER (blue solid curve) and WER (blue dashed curve) for a length 10^5 rate 0.02, ME-LDPC code with degree distribution from [13] with a maximum of 5,000 decoder iterations. Here R is the code rate and s is the channel SNR. Also shown is the zero-error channel capacity for this code rate (solid black curve) and the non-zero error channel capacity for this code rate (dashed black curve).

at the given BER reduces significantly if a non-zero error rate is allowed. Also shown in Fig. 1 is the non-zero error-rate capacity. Indeed, if we consider that we are allowed to operate at error rates as high as we like, the results in [21] tell us that by operating close to the non-zero-error-rate capacity we can obtain a very large increase in SNR over the zero-error-rate capacity and thus obtain a $\beta \gg 1$. Fig. 2 shows β results we have obtained in practice for the code from Fig. 1 as the WER is varied.

In this section we have demonstrated that fixed-rate forward error correction codes operated at a non-zero WER can operate at lower SNR than ideal codes operating at a zero WER, thus returning a β above unity. Alternatively, if the SNR is fixed, operating the codes at higher WERs increases the code rate R that can be used thereby increasing the likelihood that we

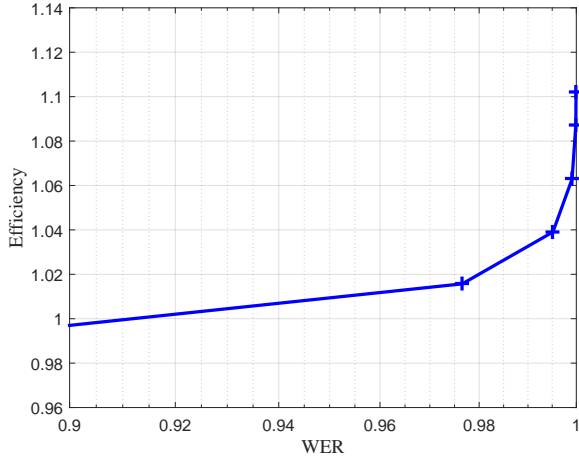


FIG. 2. The values of β , Eq. (3), obtained for the length 10^5 rate 0.02, multi-edge LDPC code with degree distribution from [13] with a maximum of 5,000 decoder iterations.

can obtain a positive $(R - I_E)$ term in the secret key model. In the following section we demonstrate that this has important consequences for the validity of the key rate model, as currently defined.

CODES WITH β GREATER THAN UNITY APPLIED TO UNITY-GAIN CLASSICAL TELEPORTER QUANTUM CHANNELS

We have demonstrated that it is possible to operate at a code rate above that of an ideal code by using, fixed-rate forward error correction codes operating at sufficiently high WERs. We will now describe a problem that arises with the secret key model in Eq. (2) when considering codes operating at a non-zero WER.

In quantum information theory, it has been shown that when a quantum channel is replaced with a classical teleporter [22], no entanglement can be transmitted through such a channel [18].

As a consequence, in the context of quantum key distribution, no secret key can be established through such a quantum channel [23]. Such a channel would be equivalent to an intercept-and-resend attack.

A Gaussian quantum channel is completely described by the channel transmission and the channel excess noise [9].

In the case where a quantum channel is replaced by a classical teleporter operating at unitary gain [22], the quantum channel parameters are described by a transmission $T = 1$ and a (relative input) excess noise of $\varepsilon = 2$.

From Eq. ((2)), we can see that the secret key model

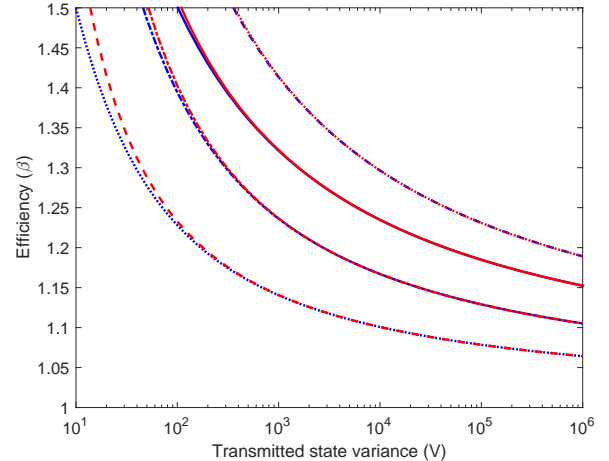


FIG. 3. The β required to achieve a positive secret key rate for a unity-gain classical teleporter quantum channel for various Gaussian CVQKD protocol configurations: Direct reconciliation (blue) and reverse reconciliation (red); Squeezed states and homodyne detection (solid line); coherent states and homodyne detection (dotted line); coherent states and heterodyne detection (dot-dashed line); squeezed states and heterodyne detection (dashed line). β is plotted versus Alice's transmitted state variance (V).

is positive when

$$\beta > \frac{I_E}{I_{AB}}, \quad (14)$$

this is equivalent to $R > I_E$ from the previous section. We can therefore calculate the β required to achieve a positive rate in the secret key model.

Fig. 3 shows the value of β required to achieve a positive secret key for the following CVQKD protocols: coherent or squeezed state sources; homodyne or heterodyne detection; and direct and reverse reconciliation protocols (For details see Ref [24]). In Fig. 3, we have assumed collective attacks, asymptotic key lengths, and ideal detection efficiency. An example of the equations describing the channel capacity (I_{AB}) and Eve's maximum accessible information (I_E) are detailed in Appendix 1. Fig. 3 plots the required β versus Alice's transmitted state variance ($V = V_A + 1$), which is the only free parameter and is normalized to the quantum noise limit.

Fig. 3 shows that β s only slightly greater than unity are required to achieve a positive key rate for a number of Gaussian CVQKD protocols operating over unity-gain classical teleporter quantum channel. In the previous section we demonstrated that the secret key rate model Eq. (1) can lead to greater than unity β . This is in addition to recent advances in Gaussian to binary mapping protocols have demonstrated high efficiencies at low-SNR ratios (For example see Ref [19]). Finally, we note that greater β_{FEC} values could be obtained by

operating poorer FEC codes, poorer in the sense of a slower drop off in error rate with increasing SNR above capacity, as these codes can also have a slower increase in error rate with decreasing SNR below capacity.

A DISCUSSION ON THE SECRET KEY RATE MODEL

In the previous section we demonstrated that the secret key rate models given by in Eq. (2) and Eq. (5) give incorrect results when employing fixed-rate forward error correction and operating over a range of high WERs. It is logical to reason that the secret key rate models may then be incorrect for all non-zero WERs. And since applications of fixed-rate ME-LDPC codes are operated at quite high WERs, it is logical to conclude that the secret key model is incorrect when such codes are used in the error reconciliation procedure [10–15].

In the following we discuss how the current secret key rate model may be incorrect.

A CVQKD post-selection perspective

Here we make the observation that the act of choosing which codewords to keep or discard based on their decoding performance is equivalent to a form of post-selection. In a general CVQKD post-selection protocol, Alice and Bob discard a subset of their data in-order to gain an information advantage over Eve. Likewise, in an error reconciliation process, Alice and Bob “post-select” the transmitted words that decoded to correct codewords and discard those that did not.

A secret key rate model has been proposed in the context of the CVQKD post-selection protocol [25]. The secret key rate model for a general protocol with post-selection is [16]

$$\Delta I_{PS} = f\beta I_{AB} - I_E \quad (15)$$

where f is the fraction of post-selected data. This secret key rate model is not known to be tight and can be treated a pessimistic lower bound [16]. In the forward error correction context, the selected data is the set of codewords that have been decoded to a valid codeword and so a failure rate of p_{fail} results in the fraction $f = 1 - p_{\text{fail}}$ of the transmitted codewords being post selected, which gives a post selection key rate of

$$\Delta I' = (1 - p_{\text{fail}})\beta I_{AB} - I_E. \quad (16)$$

An interpretation of this model is that all of Eve’s information is retained and distilled into remaining key bits after error correction in the case of the finite failure probability of the forward error correction system.

We consider the performance of ME-LDPC codes as the reconciliation step in a CVQKD system as described in [13, Figure 5] using both the traditional secret key model Eq. (2) and the post-selection secret key model Eq. (16).

Fig. 4 shows the secret key models (Eq. (2) and Eq. (16)) assuming collective attacks and employing reverse reconciliation, Gaussian modulated coherent states and homodyne detection. Both models utilize six ME-LDPC codes in the reconciliation procedure with performance data points $(R, s, \text{WER}, \beta)$ as reported in [13] and choose the value of signal variance, $1 < V_A < 100$ corresponding to the given SNR, s . In short, we have simply applied the same six data points from [13] to both Eq. (2) and Eq. (16) using the same CVQKD parameters in Ref. [13].

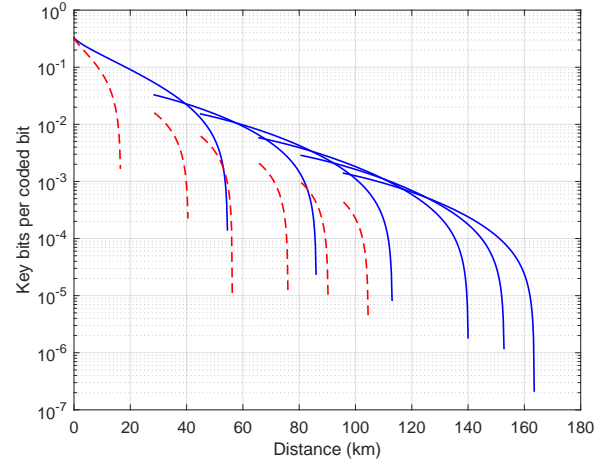


FIG. 4. Secret key models assuming collective attacks and employing ME-LDPC codes in the reconciliation procedure. The CVQKD protocol assumes reverse reconciliation, Gaussian modulated coherent states and homodyne detection. Same CVQKD parameters as Ref. [13]: $V_A \in \{1, 100\}$ modulation variance; $\varepsilon = 0.01$ relative input channel excess noise; $\eta = 0.6$ homodyne efficiency; $\nu_{\text{el}} = 0.01$ detector electronic noise; $\text{WER} = 1/3$. Solid blue: key rate model Eq. (2), dashed red: key rate model Eq. (16). From right to left the ME-LDPC code parameters $(R, s, \text{WER}, \beta)$, are [13] $(0.005, 0.00725, 0.33, 0.959)$, $(0.01, 0.0145, 0.33, 0.966)$, $(0.02, 0.029, 0.33, 0.969)$, $(0.05, 0.075, 0.33, 0.958)$, $(0.1, 0.161, 0.33, 0.931)$ and $(0.5, 1.097, 0.33, 0.936)$. There is no dashed red curve shown for the $(0.005, 0.00725, 0.33, 0.959)$ code as the key rate equation Eq. (16) returns zero key bits for this code.

Fig. 4 shows the impact of a high-WER on both the secret key rate and operational range of the secret key model Eq. (16) with a high WER impacts both the secret key rate and operational range of the protocol. This suggests that it may be better to operate the FEC codes at a much lower WER to maximize performance.

To examine this further, Fig. 5 shows the effect on the

key rate calculation for a set of ME-LDPC codes when we jointly optimized over SNR, WER and code rate. The CVQKD system is the same as described above for Fig. 4. We consider ME-LDPC codes with length 10^5 and rates 0.5, 0.1, 0.05, 0.02, and 0.005 with degree distributions as in [13]. For simplicity, we have assumed zero loss in efficiency due to Gaussian to binary mapping, have ignored finite length effects in all cases and have not placed any limitation on V_A . To obtain the values for SNR and WER for each code we simulated their performance on the BI-AWGN channel over a range of SNRs and WERs (see Appendix 2 for more detail on the optimization of the parameters).

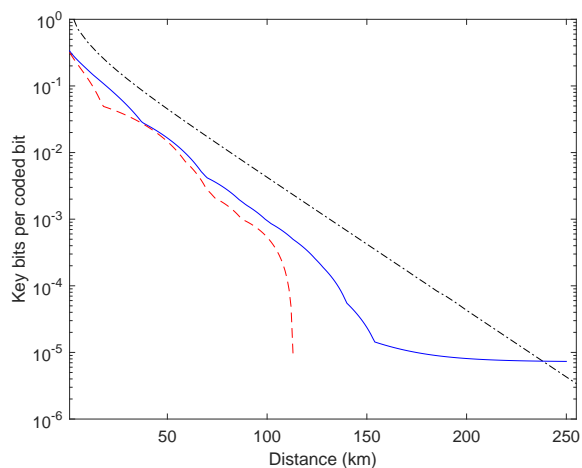


FIG. 5. Secret key models assuming collective attacks and employing ME-LDPC codes in the reconciliation procedure. Same CVQKD parameters as Fig. 4. The key rate models have been optimized over all $(R, s, \text{WER}, \beta)$ points for the six ME-LDPC codes. The ME-LDPC codes with length 10^5 bits and rates 0.5, 0.1, 0.05, 0.02, 0.01, and 0.005 are constructed randomly with degree distributions as given in [13]. The dash-dot black curve gives the key rate for a theoretically optimal code ($\beta = 1$, $\text{WER} = 0$). The solid blue curve gives the key rate calculated traditionally via Eq. (2) while the dashed red curve gives the key rate calculated via Eq. (16). See Appendix 2 for more information on the data used to generate these curves.

Fig. 5 emphasizes the problem with the secret key model Eq. (2). For high transmission losses, the optimized key rate corresponds to a high-WER with β above 1. This corresponds to a better key rate than a theoretically optimal code ($\beta = 1$, $\text{WER} = 0$). In contrast, Fig. 5 shows the secret key model Eq. (16). The secret key rate for this model is optimized at significantly lower WERs with codes operating at lower β values. We emphasize that the secret key model Eq. (16) is a conservative model of the secret key rate.

Operating at low word error rates

Increasing the WER allows us to increase the code rate R above I_{AB} thereby giving a positive

$$\beta I_{AB} - I_E = R - I_E,$$

term even when $I_{AB} < I_E$. The multiplicative correction term $(1 - \text{WER})$ simply scales down the key rate leaving it positive.

As we showed in Fig. 1, the error rate permitted has a significant effect on the code rate that can be achieved if it is allowed to be large. Of interest would be the operation of the forward error correction codes at error rates low enough so that the difference between the two cases is negligible. For ME-LDPC codes this means operating each code at a lower SNR or equivalently operating a much lower rate code at the same SNR. As an example, Fig. 6 shows the key rate we can obtain by using the same codes as the previous examples but limiting their operation to SNRs where the WER is below 0.05. Despite still allowing a quite high WER, a significant key rate loss is observed. This indicates that the high WER allowed previously played an important role in reporting good key rates.

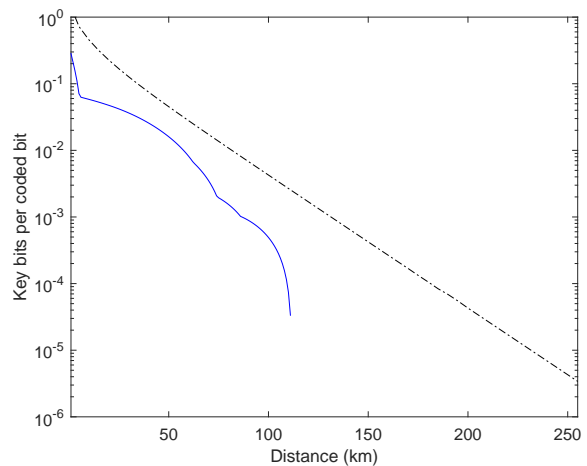


FIG. 6. Secret key models assuming collective attacks and employing ME-LDPC codes in the reconciliation procedure. Same CVQKD parameters as Fig. 4. The key rate models have been optimized over all $(R, s, \text{WER}, \beta)$ points such that $\text{WER} < 0.05$ for the six ME-LDPC codes. The ME-LDPC codes with length 100,000 bits and rates 0.5, 0.1, 0.05, 0.02, 0.01, and 0.005 are constructed randomly with degree distributions as given in [13]. The dash-dot black curve gives the key rate for a theoretically optimal code ($\beta = 1$, $\text{WER} = 0$). The solid red curve gives the key rate calculated traditionally via Eq. (2).

While it may be possible, through good code design, to improve the code WER performance of ME-LDPC codes to some extent, for fixed rate codes there will always be

a trade-off between operating at a SNR that returns a good efficiency and operating at an SNR that returns a low word error rate. Nevertheless, there are alternative forward error correction strategies that do not use fixed-rate forward error correction codes. Instead we can employ so-called rateless Raptor codes that adjust the code rate in real time so as to always decode to a valid codeword, returning codes with both low word error rates and high efficiencies.

Raptor codes are graph based codes formed from the concatenation of a high rate LDPC code with a Luby Transform (LT) code. LT codes [26] have very simple encoding and decoding processes and can approach the capacity of binary erasure channels with an unknown erasure rate. The encoding and decoding of Raptor codes are linear in terms of the message length; thus practical for applications with large data transmission. Raptor codes were studied for AWGN channels in [27], where a systematic framework was proposed to find the optimal degree distribution across a range of SNRs. The design of very low rate Raptor codes was studied in [28]. Using Raptor codes, a potentially limitless number of coded symbols can be generated, allowing the receiver to decode the message once a sufficient number of parity bits have been received; thus always decoding to a valid codeword.

It has been shown [29] that low-rate Raptor codes can achieve higher efficiencies in comparison with the fixed rate ME-LDPC codes in the entire SNR range and do so at very low WERs. When applied to the reconciliation step of CVQKD, Raptor codes can significantly improve the key rate [29]. For example, Figure 7 shows the key rate of the same CV-QKD system as considered in Fig. 4 applying the Raptor codes from [27, 29] (See Appendix 3 for more detail). For the Raptor codes the two models Eq. (16) and Eq. (2) return the same key-rate.

A new model

A full solution to this problem is non-trivial because the model involves finite-size effects (ie imperfect error correction) and asymptotic quantities. Such a solution would require a model of the number of bits revealed during the reconciliation procedure based on the particular code used, and how this quantity behaves in the asymptotic limit.

Protocols with a complete security proof in the finite-size regimes exist, for instance [30]. Such proofs for reconciliation using forward error correction will require a model of the number of bits leaked during the forward error correction reconciliation procedure as a function of the WER, and any uncertainty in it, as well as the code-word length and measurement errors.

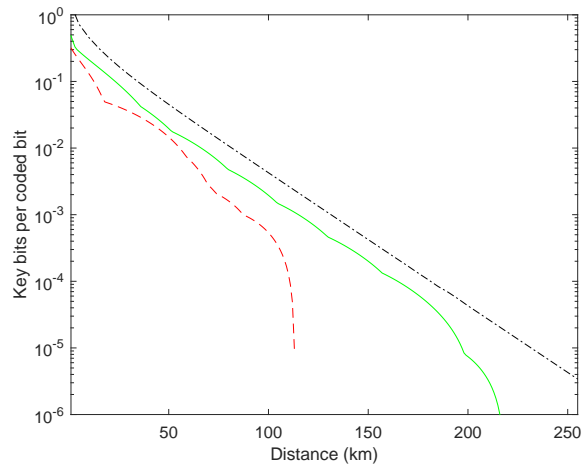


FIG. 7. Secret key models assuming collective attacks and employing for Raptor and ME-LDPC codes in the reconciliation procedure. Same CVQKD parameters as Fig. 4. For both ME-LDPC and Raptor codes, the secret key rate model has been optimized over the parameters $(R, s, \text{WER}, \beta)$. The ME-LDPC codes with codeword length $n = 10^5$ bits and rates 0.5, 0.1, 0.05, 0.02, 0.01, and 0.005 are constructed randomly with degree distributions as given in [13]. The raptor codes with message length $k = 10^4$ are constructed randomly with degree distributions as given in Appendix 3. The dash-dot black curve gives the key rate for a theoretically optimal code ($\beta = 1$, $\text{WER} = 0$). Solid green curve: the key rate model for Raptor codes via Eq. (16). Dashed red curve: key rate model for ME-LDPC codes via Eq. (16).

CONCLUSION

The maximum operation range of continuous variable quantum key distribution systems has shown to be improved by employing high-efficiency forward error correction codes such as ME-LDPC codes. In the current literature, CVQKD protocols with fixed-rate forward error correction codes typically use a modified secret key model Eq. (2) that includes the WER term.

In this paper, we have demonstrated that this secret key model is incorrect. We demonstrated this in two steps. Firstly, we showed that previously used ME-LDPC codes for a range of high word error rates, exhibited efficiencies greater than unity. Secondly, we showed that assuming that code efficiencies could be greater than unity, then using the secret key model Eq. (2), it was possible to achieve a positive secret key over an entanglement breaking channel, which is equivalent to an intercept and resend attack - an impossible scenario. We concluded that if the secret key model is incorrect for a range of high WERs, it is also possibly incorrect for any non-zero WERs.

We subsequently discussed the secret key model from the perspective of CVQKD post-selection protocols. In a CVQKD post-selection protocol, Alice and Bob discard

a subset of their data in-order to gain an information advantage over Eve. Similarly, in an error reconciliation process, Alice and Bob “post-select” the code words that decoded to valid codewords and discard codewords that they were unable to decode. This secret key rate model is not known to be tight but can be treated as a lower bound [16]. We showed that using the post selection key rate model reduces the previously reported operational range of such CVQKD systems employing fixed length forward error correction codes. We also showed that using the current secret key rate model, but restricting the codes to operate at lower WERs, can also reduce the previously reported operational range of CVQKD systems employing fixed length forward error correction codes. However, we did show that it is possible to employ an alternative forward error correction coding solution in the form of Raptor codes, which provide high efficiencies while operating at very low WERs.

A full solution to this problem would require a model of the number of bits revealed during the reconciliation procedure based on the particular code used, and how this quantity behaves in the asymptotic limit. Until such a model is known we would suggest that key rates obtained using the current model while operating at high WERs may not be accurate.

Acknowledgments

Financial support was provided to A.M.L, T.S & S.J.J. through the Australian Research Council Linkage Projects (Project ID LP130100783). S.J.J and L.O. are supported by the Australian Research Council via Future Fellowships (FT110100195 and FT140100219 respectively).

APPENDIX 1

In this section we detail Alice and Bob’s channel capacity as well as Eve’s information for the Gaussian protocol with reverse reconciliation and employing coherent states and homodyne detection. Here we assume collective attacks and asymptotic key lengths. The free parameters in these equations are the following: V variance of the transmitted state; T quantum channel with transmission; ε relative input channel excess noise; η homodyne efficiency; ν_{el} detector electronic noise. Alice and Bob’s channel capacity (I_{AB}) and Eve’s information (I_{E}) are described by the following compact set of equations [31].

$$I_{\text{AB}} = C = \frac{1}{2} \log_2 \left(\frac{V + \chi_{\text{tot}}}{\chi_{\text{tot}} + 1} \right) \quad (17)$$

$$V = V_{\text{A}} + 1 \quad (18)$$

$$\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/T \quad (19)$$

$$\chi_{\text{line}} = 1/T - 1 + \varepsilon \quad (20)$$

$$\chi_{\text{hom}} = (1 - \eta + \nu_{\text{el}})/\eta \quad (21)$$

$$I_{\text{E}} = G[(\lambda_1 - 1)/2] + G[(\lambda_2 - 1)/2] \quad (22)$$

$$-G[(\lambda_3 - 1)/2] - G[(\lambda_4 - 1)/2] \quad (23)$$

$$G[x] = (x + 1) \log_2(x + 1) - x \log_2(x) \quad (24)$$

$$\lambda_1 = \sqrt{\frac{1}{2} \left(A + \sqrt{A^2 - 4B} \right)} \quad (25)$$

$$\lambda_2 = \sqrt{\frac{1}{2} \left(A - \sqrt{A^2 - 4B} \right)} \quad (26)$$

$$\lambda_3 = \sqrt{\frac{1}{2} \left(C + \sqrt{C^2 - 4D} \right)} \quad (27)$$

$$\lambda_4 = \sqrt{\frac{1}{2} \left(C - \sqrt{C^2 - 4D} \right)} \quad (28)$$

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{\text{line}})^2 \quad (29)$$

$$B = T^2(V + \chi_{\text{line}} + 1)^2 \quad (30)$$

$$C = \frac{A\chi_{\text{hom}} + V\sqrt{B} + T(V + \chi_{\text{line}})}{T(V + \chi_{\text{line}})} \quad (31)$$

$$D = \sqrt{B} \frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{\text{line}})} \quad (32)$$

$$(33)$$

The complete set of Gaussian protocol configurations, includes: squeezed states and homodyne detection; coherent states and heterodyne detection and squeezed states and heterodyne detection. These protocols are described in detail elsewhere [24] in the case of ideal homodyne detector efficiency and ideal forward error correction codes.

APPENDIX 2

In this section we provide details for optimizing the secret key rate models shown in Fig. 5. We consider ME-LDPC codes with length 100,000 and rates 0.5, 0.1, 0.05, 0.02, and 0.005 with degree distributions as in [13]. The parity-check matrices were constructed randomly subject to the degree distribution constraints. Fig. 8 shows the performance of the ME-LDPC codes with rates 0.005, 0.01, 0.02, 0.05, 0.1 as the channel SNR is varied.

We then jointly optimized over SNR, WER and rate to maximize the secret key rate for each transmission distance. The final secret key rate is the maximum key rate over all codes. In Figs. 9 to 12, the solid red curves give

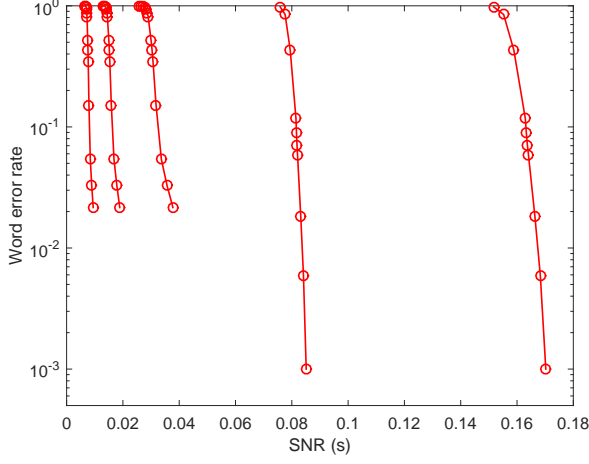


FIG. 8. WER versus SNR for the considered ME-LDPC codes. From left to right are the ME-LDPC codes with rates 0.005, 0.01, 0.02, 0.05, 0.1.

the parameters which optimize the key rate calculated via Eq. (2) while the dashed red curves give the parameters which optimize the key rate calculated via Eq. (16).

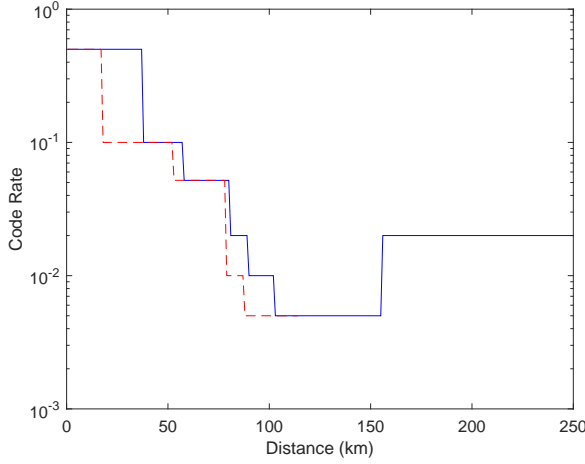


FIG. 9. Optimized code rate versus distance for key rate equations Eq. (2) (solid blue) compared to key rate equations Eq. (16) (dashed red curve)

APPENDIX 3

We consider two Raptor codes in this paper. The first code, from [28], has degree distribution

$$\begin{aligned} \Omega(x) = & 0.0035x + 0.3538x^2 + 0.2337x^3 + 0.0737x^4 \\ & + 0.0755x^5 + 0.0262x^6 + 0.0608x^7 + 0.0493x^{11} \\ & + 0.0255x^{12} + 0.0002x^{21} + 0.0454x^{23} \\ & + 0.0072x^{57} + 0.0180x^{58} + 0.0272x^{300} \end{aligned} \quad (34)$$

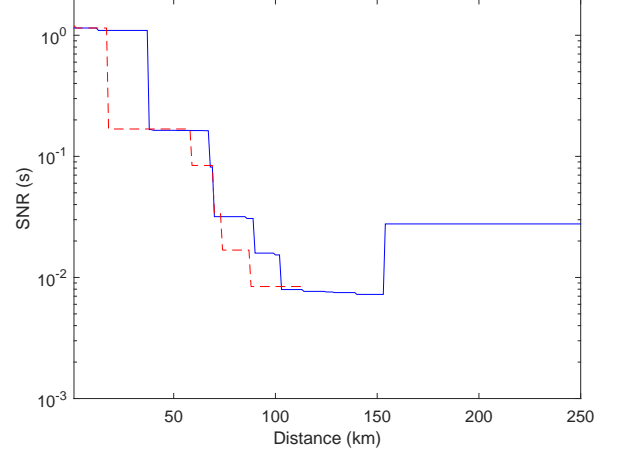


FIG. 10. Optimized SNR versus distance for key rate equations Eq. (2) (solid blue) compared to key rate equations Eq. (16) (dashed red curve)

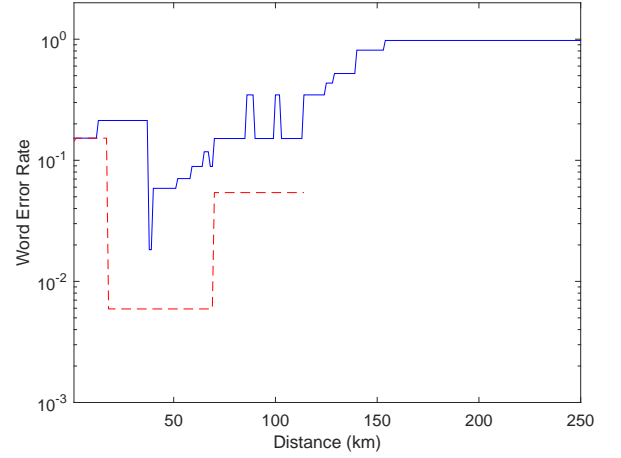


FIG. 11. Optimized WER versus distance for key rate equations Eq. (2) (solid blue) compared to key rate equations Eq. (16) (dashed red curve)

The second Raptor code, from [27], has degree distribution

$$\begin{aligned} \Omega(x) = & 0.0146x^1 + 0.3766x^2 + 0.0677x^3 + 0.2946x^4 \\ & + 0.1291x^9 + 0.0060x^{12} + 0.0341x^{24} + 0.0228x^{29} \\ & + 0.0073x^{43} + 0.0472x^{200} \end{aligned} \quad (35)$$

See [27, 28] for details on encoding and decoding algorithms for these codes. Figure 13 shows the simulated efficiency for these codes on an AWGN channel as the SNR is varied.

* sarah.johnson@newcastle.edu.au

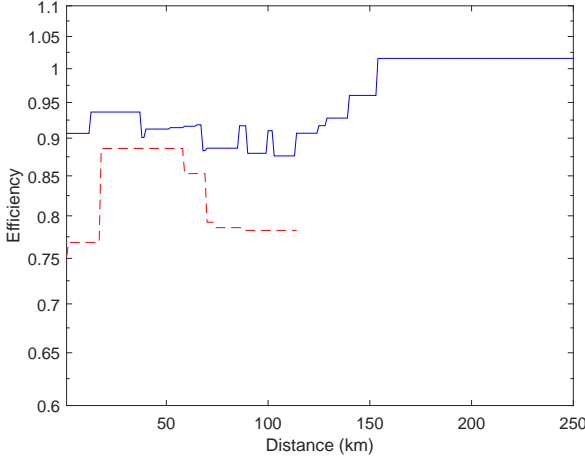


FIG. 12. Optimized β versus distance for key rate equations Eq. (2) (solid blue) compared to key rate equations Eq. (16) (dashed red curve)

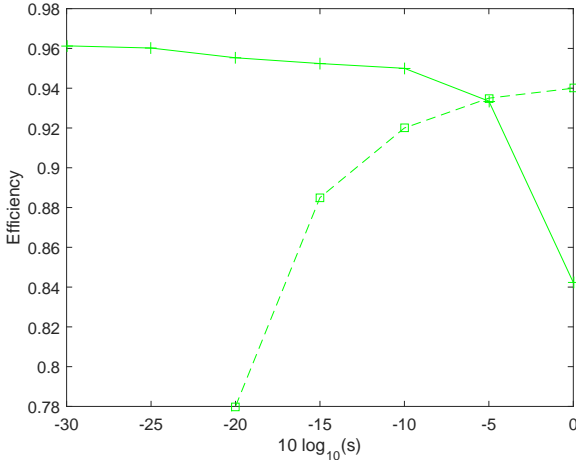


FIG. 13. β versus SNR for the two raptor codes. The solid curve gives β values obtained for the code from [28] with degree distribution (34) and message length $k = 100,000$. The dashed curve gives the efficiency of the code from [27] with degree distribution (35) and message length $k = 38,000$.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009. [Online]. Available: <http://link.aps.org/doi/10.1103/RevModPhys.81.1301>

[3] C. Weedbrook, S. Pirandola, R. García-Patrón, N. Cerf, T. Ralph, J. Shapiro, and S. Lloyd, “Gaussian quantum information,” *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, 2012.

[4] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics*, vol. 8, p. 595604,

2014.

[5] R. García-Patrón and N. Cerf, “Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution,” *Phys. Rev. Lett.*, vol. 97, p. 190503, 2006.

[6] M. Navascués, F. Grosshans, and A. Acín, “Optimality of Gaussian attacks in continuous-variable quantum cryptography,” *Phys. Rev. Lett.*, vol. 97, p. 190502, 2006.

[7] A. Leverrier, “Composable security proof for continuous-variable quantum key distribution with coherent states,” *Phys. Rev. Lett.*, vol. 114, p. 070501, Sep 2008. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevLett.109.100502>

[8] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002.

[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, “Quantum key distribution using Gaussian-modulated coherent states,” *Nature*, vol. 421, p. 238, 2003.

[10] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, “Quantum key distribution over 25 km with an all-fiber continuous-variable system,” *Phys. Rev. A*, vol. 76, p. 042305, Oct 2007. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.76.042305>

[11] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, “Field test of a continuous-variable quantum key distribution prototype,” *New J. Phys.*, vol. 11, p. 045023 (14pp), 2009, doi:10.1088/1367-2630/11/4/045023.

[12] A. Leverrier and P. Grangier, “Conditional security proof of long distance continuous-variable quantum key distribution with discrete modulation,” *Phys. Rev. A*, vol. 102, p. 180504, 2009.

[13] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, “Long distance continuous-variable quantum-key-distribution protocols with a Gaussian modulation,” *Phys. Rev. A*, vol. 84, p. 062317, 2011.

[14] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” *Nature Photon.*, vol. 7, pp. 378–381, 2013.

[15] D. L. Duan Huang, Peng Huang and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” *Scientific Reports*, vol. 6, no. 19201, 2016.

[16] A. Leverrier, “Theoretical study of continuous-variable quantum key distribution,” 2009, PhD Thesis, ParisTech.

[17] J. Martinez-Mateo, D. Elkouss, and V. Martin, “Key reconciliation for high performance quantum key distribution,” *Scientific Reports*, vol. 3, 2013.

[18] F. Grosshans, N. Cerf, P. Grangier, J. Wenger, and R. Tualle-Brouri, “Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables,” *Quantum Inf. Comput.*, vol. 3, p. 535, 2003.

[19] A. Leverrier, R. Allame, J. Boutros, G. Zmor, and P. Grangier, “Multidimensional reconciliation for a continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 77, p. 042325, 2008.

[20] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, “Design of capacity-approaching irregular low-density parity-check codes,” *IEEE Trans. Inform. The-*

- ory, vol. 47, no. 2, pp. 619–637, Feb. 2001.
- [21] J. P. Aldis, “Capacity of digital communication system with allowed nonzero error rate,” *Electronics Letters*, vol. 28, no. 13, pp. 1252–1253, June 1992.
 - [22] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, “Unconditional quantum teleportation,” *Science*, vol. 282, no. 5389, pp. 706–709, 1998.
 - [23] M. Curty, M. Lewenstein, and N. Lütkenhaus, “Entanglement as precondition for secure quantum key distribution,” *Phys. Rev. Lett.*, vol. 92, p. 217903, 2004.
 - [24] R. García-Patrón, “Quantum information with optical continuous variables: from bell tests to key distribution,” Ph.D. dissertation, Université libre de Bruxelles, 2007.
 - [25] N. L. Ch. Silberhorn, T. C. Ralph and G. Leuchs, “Continuous variable quantum cryptography: Beating the 3 db loss limit,” *Phys. Rev. Lett.*, vol. 89, p. 167901, 2002.
 - [26] M. Luby, “LT codes,” in *Proc. 43rd Annual IEEE Symp. Foundations Comput. Science*, Nov. 2002, pp. 271 – 280.
 - [27] O. Etesami and A. Shokrollahi, “Raptor codes on binary memoryless symmetric channels,” *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2033 – 2051, May. 2006.
 - [28] M. Shirvanimoghaddam and J. S. J., “Raptor codes in the low SNR regime,” *IEEEComms*, vol. 64, no. 11, pp. 4449–4460, Nov 2016.
 - [29] M. Shirvanimoghaddam, S. J. Johnson, and A. M. Lance, “Design of Raptor codes in the low SNR regime with applications in quantum key distribution,” in *Proc. IEEE International Communications Conference (ICC)*, May. 2016, pp. 1–6.
 - [30] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, “Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks,” *Phys. Rev. Lett.*, vol. 109, p. 100502, Sep 2012. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevLett.109.100502>
 - [31] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouiri, and P. Grainger, “Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers,” *J. Phys. B: At. Mol. Opt. Phys.*, vol. 42, p. 114014, 2009.